



*Operating System*

## End User Certificate Management

### Beta 3 Technical Walkthrough

---

#### **Abstract**

This technical walkthrough takes you through the process that end users would go through to obtain and manage certificates in the Microsoft® Windows 2000® operating system. Advanced certificate management using the Certificates Microsoft Management Console (MMC) snap-in is covered in a separate walkthrough.

© 1999 Microsoft Corporation. All rights reserved.

*THIS IS PRELIMINARY DOCUMENTATION. The information contained in this document represents the current view of Microsoft Corporation on the issues discussed as of the date of publication. Because Microsoft must respond to changing market conditions, it should not be interpreted to be a commitment on the part of Microsoft, and Microsoft cannot guarantee the accuracy of any information presented after the date of publication.*

*This BETA document is for informational purposes only. MICROSOFT MAKES NO WARRANTIES, EXPRESS OR IMPLIED, IN THIS DOCUMENT.*

*Microsoft, The Windows logo, Windows, and Windows NT are registered trademarks of Microsoft Corporation. Other product or company names mentioned herein may be the trademarks of their respective owners.*

*Microsoft Corporation • One Microsoft Way • Redmond, WA 98052-6399 • USA*

*0599*

---

## CONTENTS

INTRODUCTION .....	1
Prerequisites	1
CERTIFICATE MANAGEMENT IN WINDOWS 2000.....	2
Viewing Your Certificates	2
Installing a Root Certificate	8
Obtaining a Client Authentication Certificate from the Microsoft Test Certification Authority	12
Changing a Certificate's Intended Purposes	16
Exporting Certificates	22
Importing Certificates	28
FOR MORE INFORMATION .....	33
Before You Call for Support	33
Reporting Problems	33

---



---

## INTRODUCTION

This technical walkthrough takes you through the process that end users would go through to obtain and manage certificates in the Microsoft® Windows®2000 operating system. Advanced certificate management using the Certificates Microsoft Management Console (MMC) snapin is covered in a separate technical walkthrough.

### Prerequisites

This technical walkthrough assumes the following environment:

- You have installed Windows 2000 Professional build 1943 or later in a Windows 2000 domain.
- A Windows 2000 Certification Authority (CA) is running in the domain.

## CERTIFICATE MANAGEMENT IN WINDOWS 2000

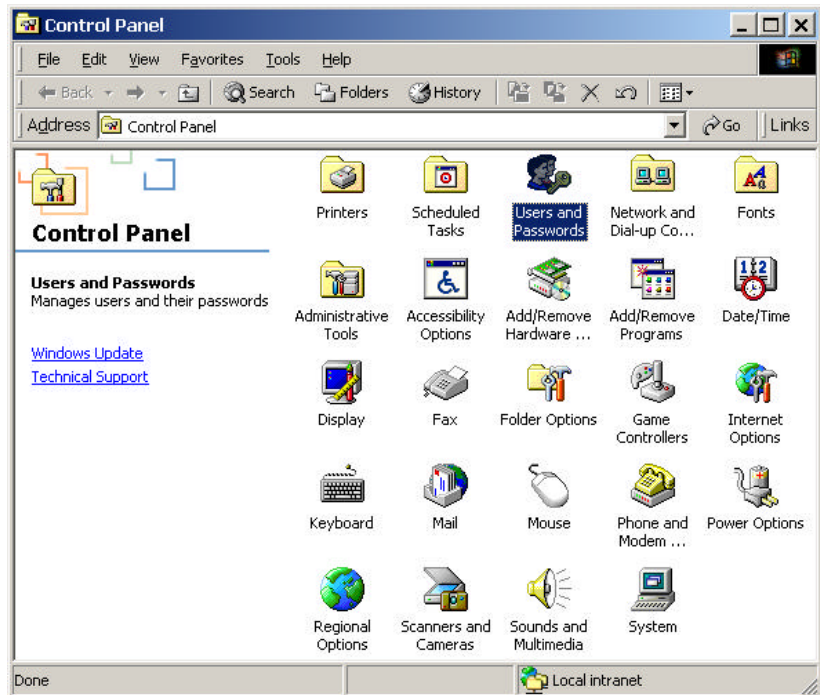
This section explains how to view and manage certificates in your certificate stores.

### Viewing Your Certificates

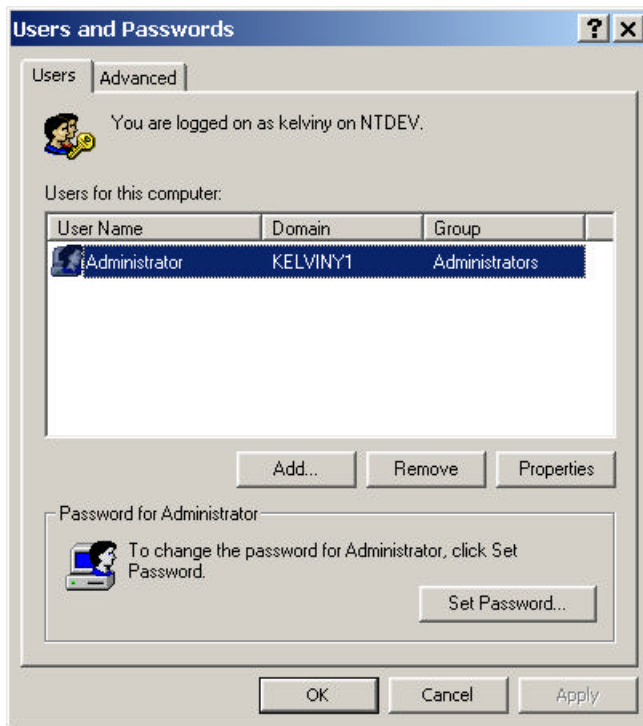
You may need to look at your certificates in the certificate stores (for example, you want to find the list of commercial CAs you trust).

#### To view your certificates

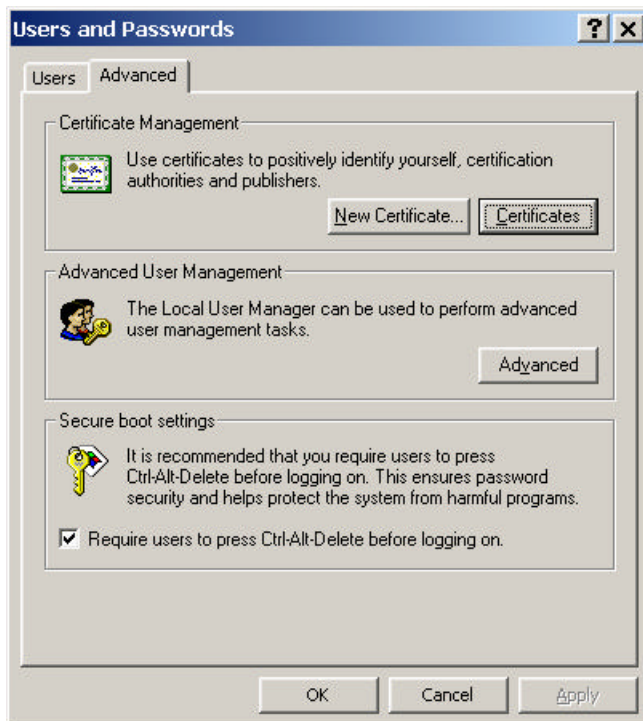
1. Open **Control Panel**.



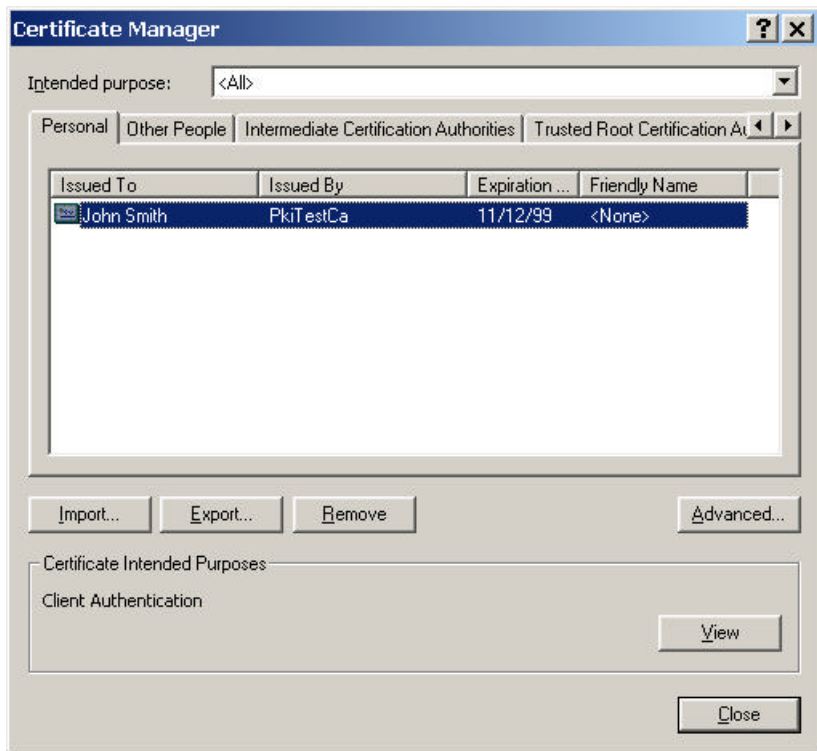
2. Double-click **Users and Passwords**. The **Users and Passwords** dialog box appears.



3. Click the **Advanced** tab. The **Advanced** property page appears.



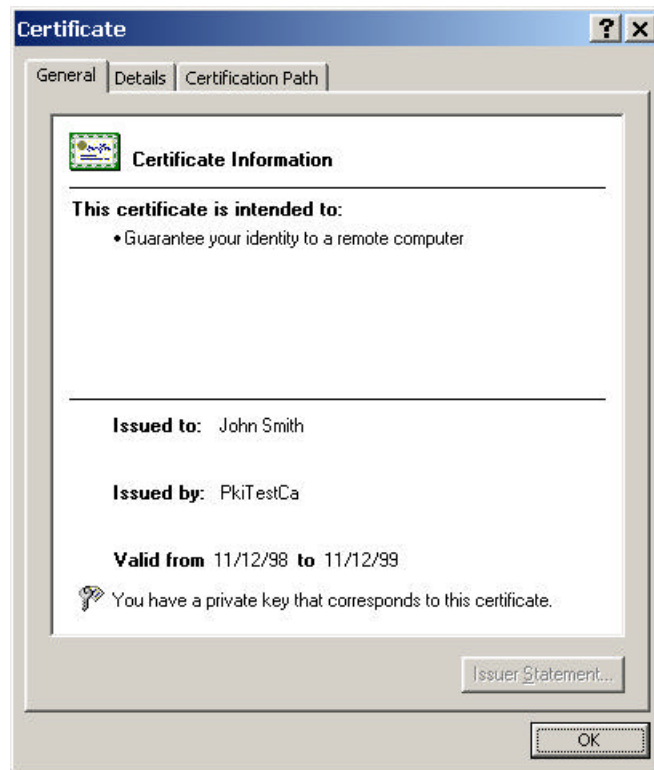
4. Click **Certificates** to start **Certificate Manager**.



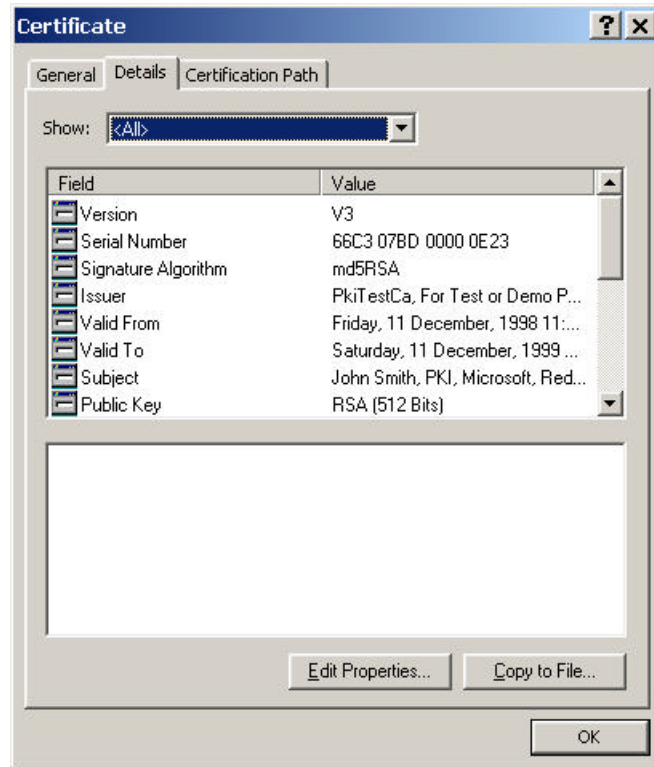
5. Certificates are organized into the following four categories. Each of the categories is a separate tab within the **Certificate Manager** dialog box.
- **Personal.** Certificates that are issued to you.
  - **Other People.** Certificates that are issued to other individuals or companies.
  - **Intermediate Certification Authorities** Certificates that are issued to certification authorities (CA). These certificates must verify up to a root certificate in the Trusted Root Certification Authorities.
  - **Trusted Root Certification Authorities** Certificates that are issued by root certification authorities that you trust explicitly.



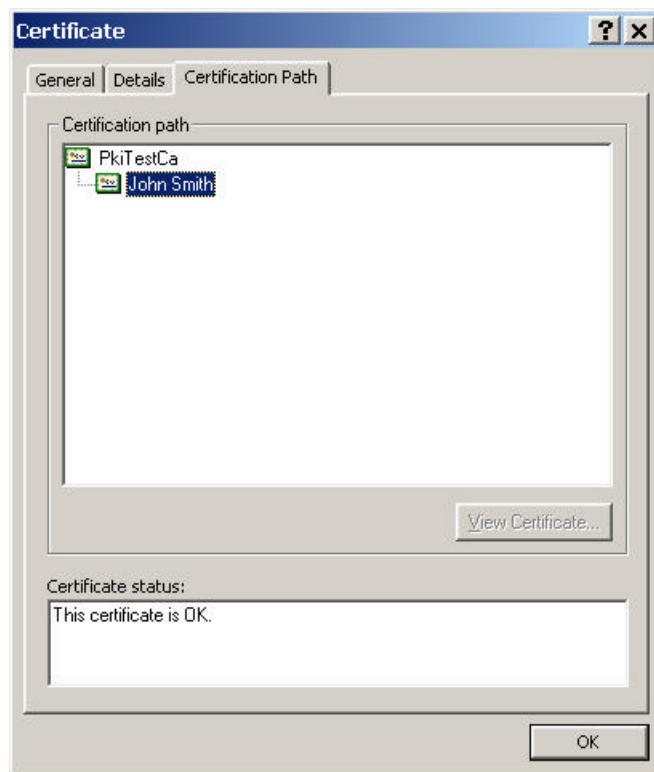
6. Double-click a certificate to view information about it. The **Certificate** dialog box is organized into three tabs:
- **General**. Default view for seeing a certificate's purposes.



- **Details.** Displays the actual X.509 fields, extensions, and properties of a certificate. You may also click **Edit Properties** in this view. This allows you to modify the *Friendly Name* and *Description* fields. You can also specify what the certificate can be used for.



- **Certification Path** Displays the certification path.



## Installing a Root Certificate

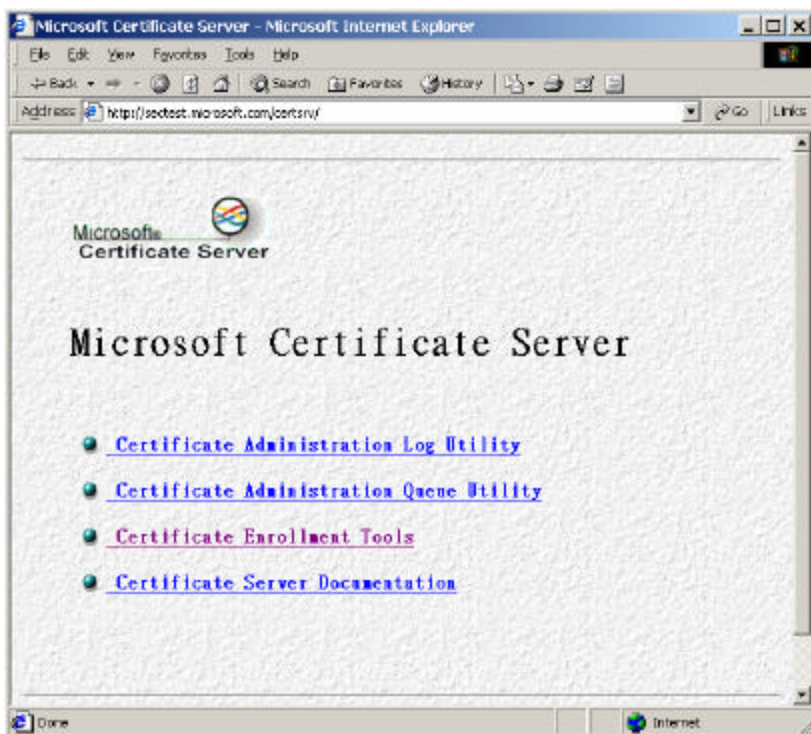
Windows 2000 has a number of pre-installed root certificates for various commercial certification authorities. If you choose to use a commercial CA that is not installed, you must install the CA root certificate to enable trust of any certificates issued by that CA. Installation of the CA root certificate may vary depending on the particular CA. This example shows you how to install the root certificate for the Microsoft test certification authority (available at <http://sectest.microsoft.com/certsrv/>).

**Note** This CA is for demonstration purposes only.

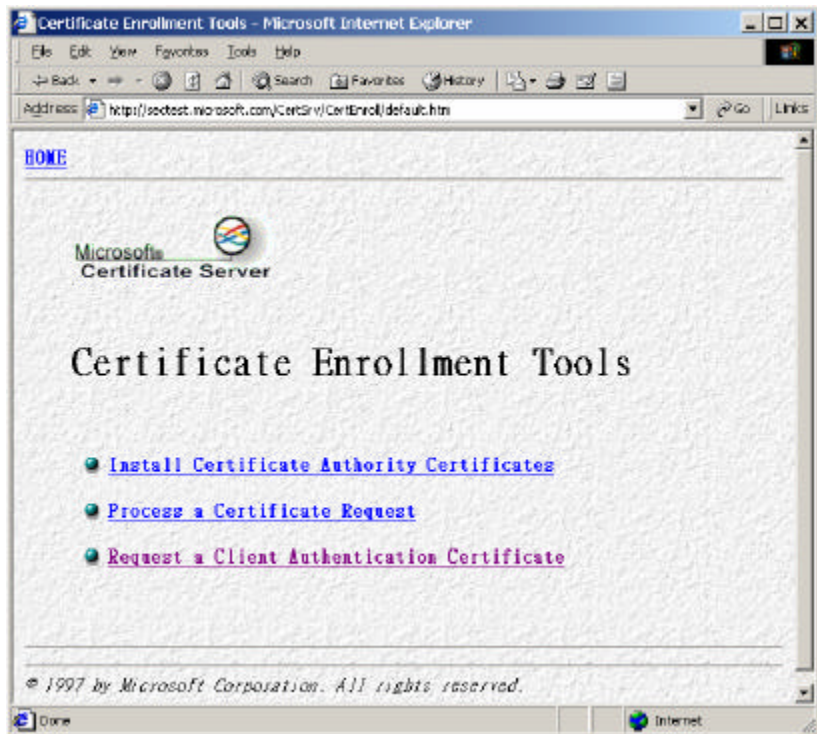
Root certificates for Windows 2000 Certification Authorities in the same domain as the client are installed automatically.

### To install a root certificate

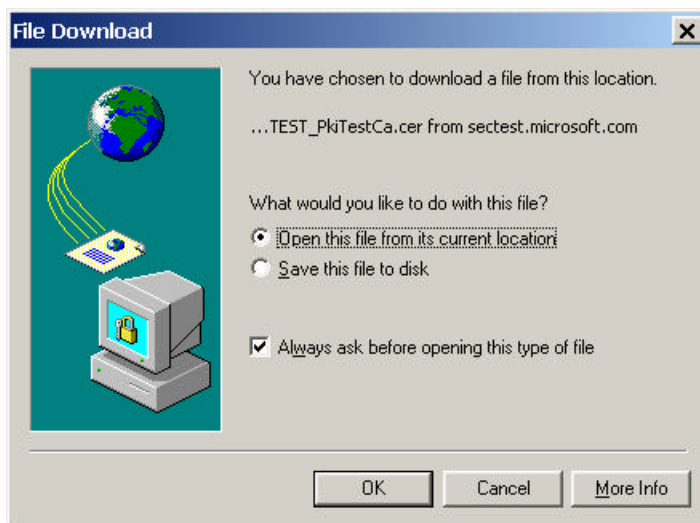
1. Connect to <http://sectest.microsoft.com/certsrv/> using Microsoft Internet Explorer.



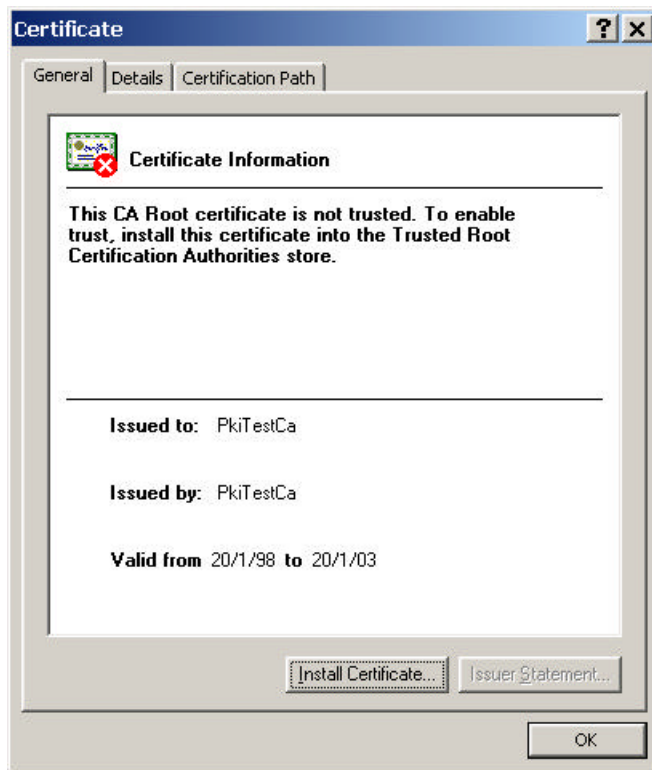
2. Click the **Certificate Enrollment Tools** link.



3. Click the **Install Certificate Authority Certificates** link.
4. Click the **Certificate for SECTESTPkiTestCA** link.
5. From the **File Download** dialog box, select **Open this file from its current location**. Click **OK**.



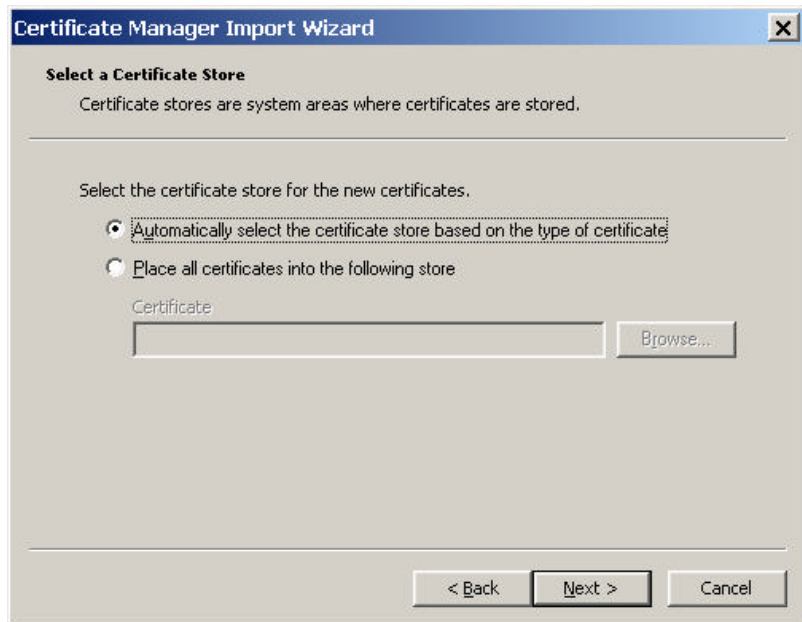
6. On the **General** tab, click **Install Certificate**



7. Click **Next**.



8. By default, the **Certificate Manager Import** wizard will import root certificates into the Trusted Root Certification Authorities certificate store. Root certificates must be in this certificate store to be trusted by the system. Click **Next**.



9. Click **Finish** to import the certificate.





## Obtaining a Client Authentication Certificate from the Microsoft Test Certification Authority

This example will show you how to get a client authentication certificate from the Microsoft test certificate authority (available at <http://sectest.microsoft.com/certsrv>) using Internet Explorer.

**Note** This CA is for demonstration purposes only.

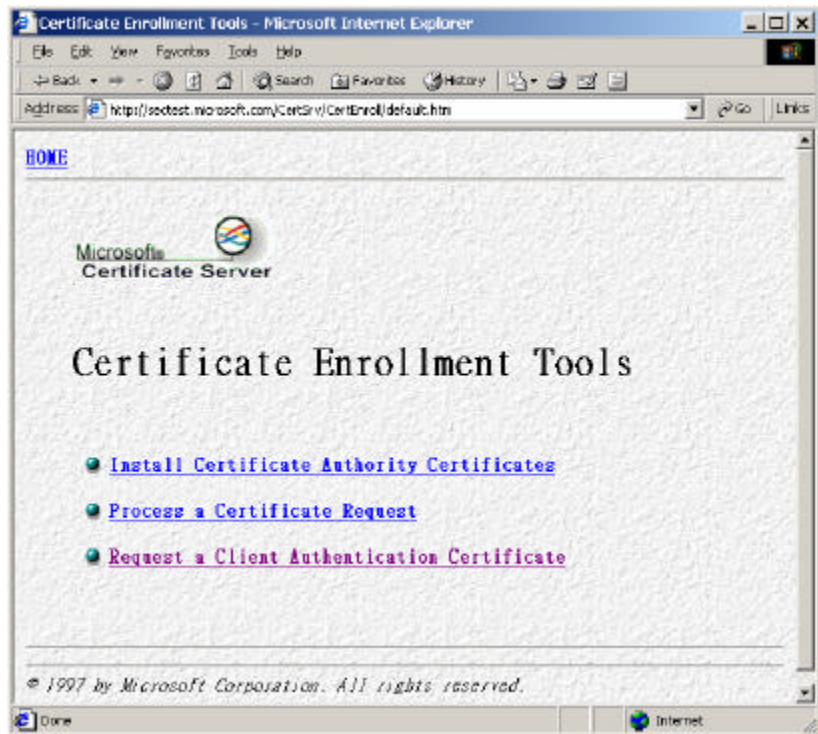
1. Go to <http://sectest.microsoft.com/certsrv>



2. Click the **Certificate Enrollment Tools** link.



3. Click the **Request a Client Authentication Certificate** link.



4. Complete the **Certificate Enrollment Form**.

The screenshot shows the 'Certificate Enrollment Form' in a Microsoft Internet Explorer window. The address bar displays 'http://sectest.microsoft.com/CertEnroll/ceenroll.asp'. The page features the Microsoft Certificate Server logo and the title 'Certificate Enrollment Form'. Below the title is a form with the following fields and values:

Name:	John Smith
Department:	PKI
Organization:	Microsoft
City:	Redmond
State:	WA
Country:	US
E-Mail:	johnsmith@microsoft.com

At the bottom of the form are two buttons: 'Submit Request' and 'Advanced'.

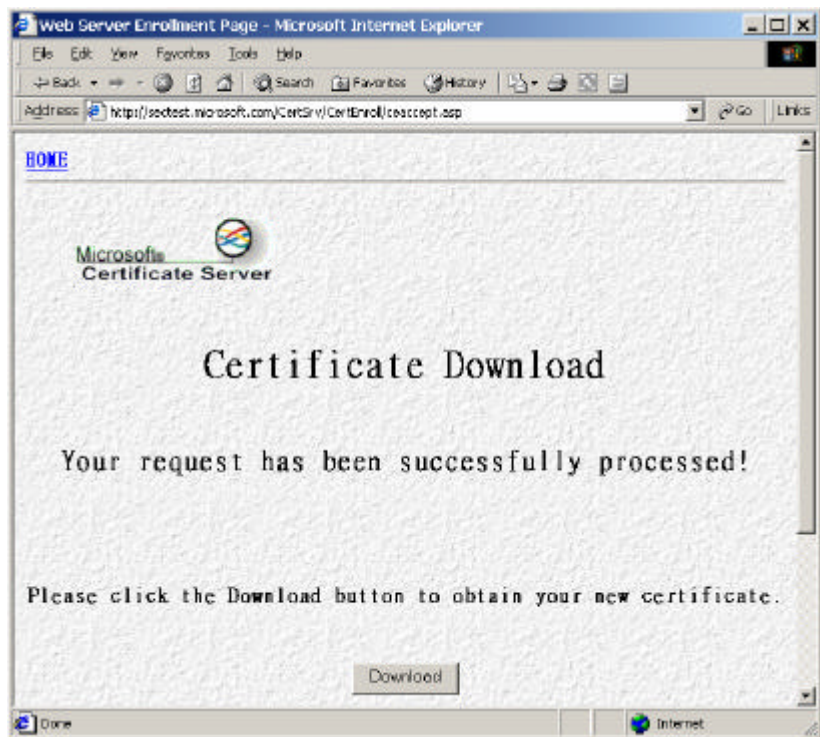
5. Click **Advanced** to edit advanced options.

The screenshot shows the 'Advanced Settings' page in a Microsoft Internet Explorer window. The address bar displays 'http://sectest.microsoft.com/CertEnroll/ceadv.asp'. The page features the Microsoft Certificate Server logo and the title 'Advanced Settings'. Below the title is a message: 'Please ensure that the CSP supports the setting you select.' The form contains the following sections:

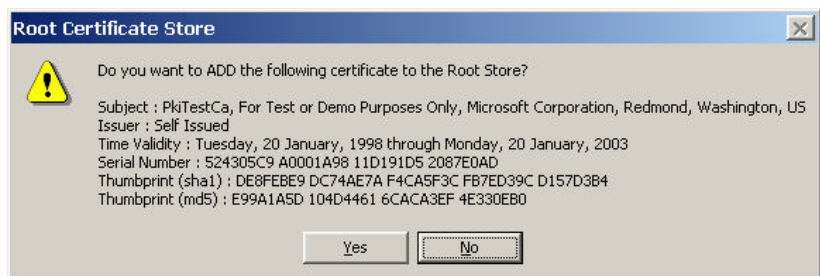
<b>Key Spec:</b> <ul style="list-style-type: none"><li><input checked="" type="radio"/> Exchange</li><li><input type="radio"/> Signature</li></ul>	<b>Properties:</b> <ul style="list-style-type: none"><li><input type="checkbox"/> Use Existing Key Set</li><li><input type="checkbox"/> Write Certificate to CSP</li><li><input type="checkbox"/> Set Container Name</li><li><input type="checkbox"/> Export Private Keys to File</li><li><input checked="" type="checkbox"/> Allow Keys to be Exported</li><li><input type="checkbox"/> Create a SPC file</li></ul>
<b>Algorithm:</b> <ul style="list-style-type: none"><li><input checked="" type="radio"/> SHA1</li><li><input type="radio"/> MD2</li><li><input type="radio"/> MD5</li></ul>	

At the bottom of the form is a 'Usage:' dropdown menu with 'ClientAuthentication' selected.

6. Within the list of *Properties*, select **Allow Keys to be Exported**
7. In this example, make sure the **Microsoft Base Cryptographic Provider 1.0** is selected as the Cryptographic Service Provider (CSP).
8. Click **OK** to return to the **Certificate Enrollment Form**.
9. Click **Submit Request**
10. Click **Download**.



11. If you have not installed the root certificate for this CA, you will see the **Root Certificate Store** dialog box. Click **Yes** to install the root certificate of the CA.



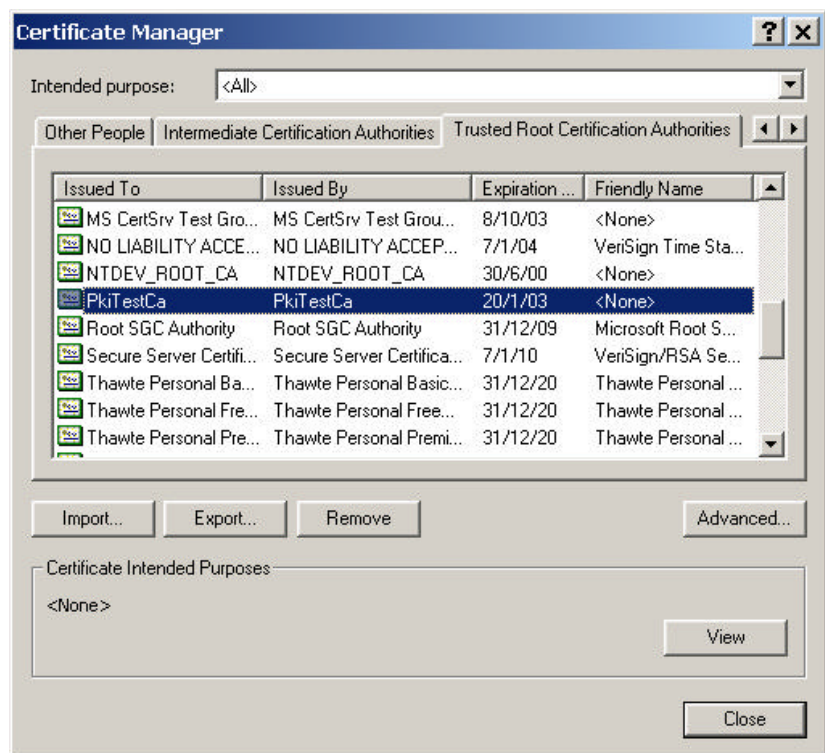
## Changing a Certificate's Intended Purposes

You may want to limit the intended purpose(s) of a certificate because certification authorities may choose to issue certificates without predefined intended purpose(s). You will be shown how to modify the intended purposes of the root certificate of Microsoft's test certification authority (available at <http://sectest.microsoft.com/certsrv>).

**Note** This CA is for demonstration purposes only.

This example assumes you have downloaded the root certificate for this CA.

1. Open **Control Panel**. Start **Certificate Manager** by double-clicking **Users and Passwords**.
2. Click the **Trusted Root Certification Authorities** tab and select **PkiTestCa**.

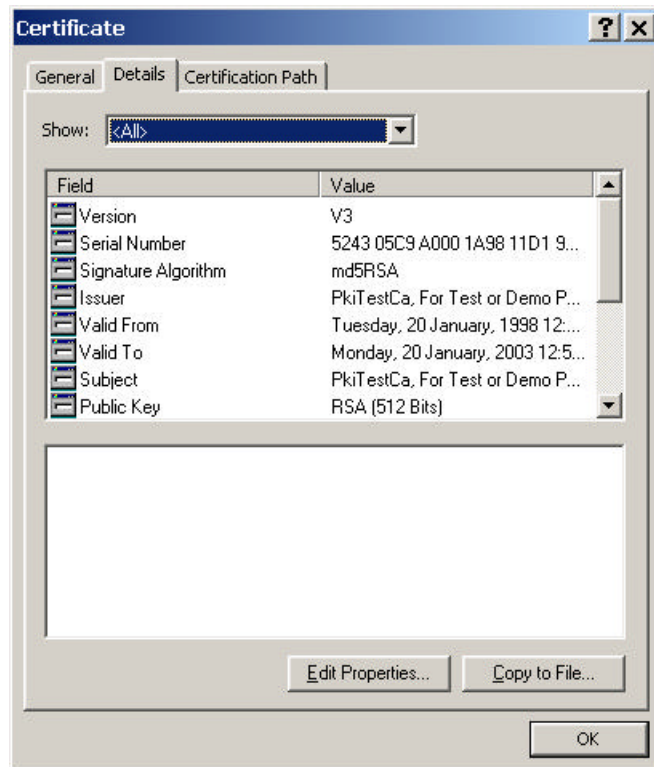


3. Click **View** to look at the detailed information in the certificate.

4. The Certificate Information is displayed on the **General** tab.

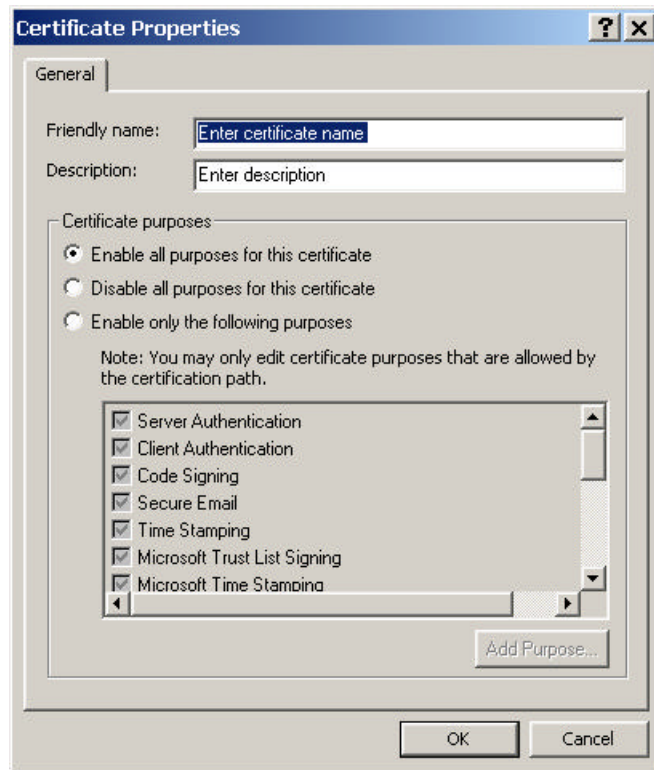


5. Select the **Details** tab. Click **Edit Properties**.

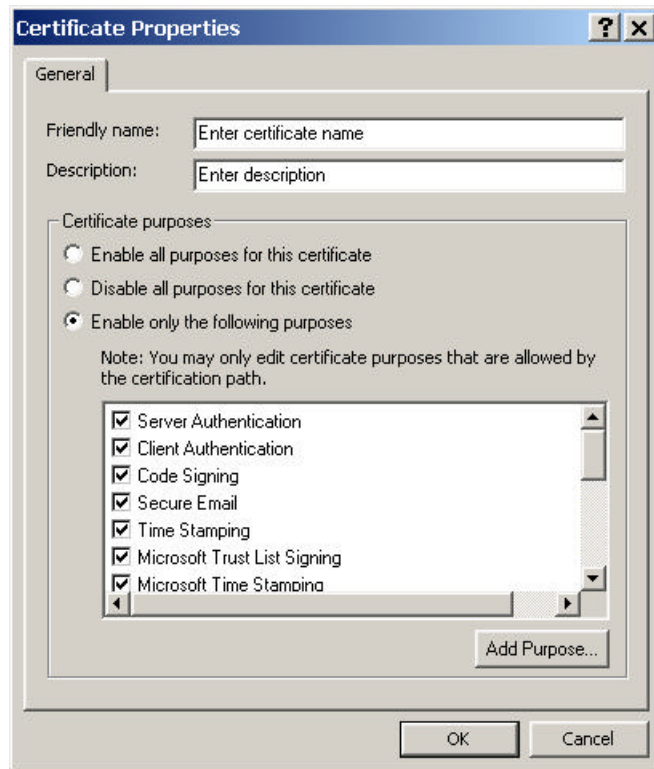




6. Within the **Certificate Properties** dialog box, note that a root certificate may contain information about its intended purpose(s). In this case, the root certificate does not contain such information. Therefore, the system will assume the certificate can be used in for purpose.

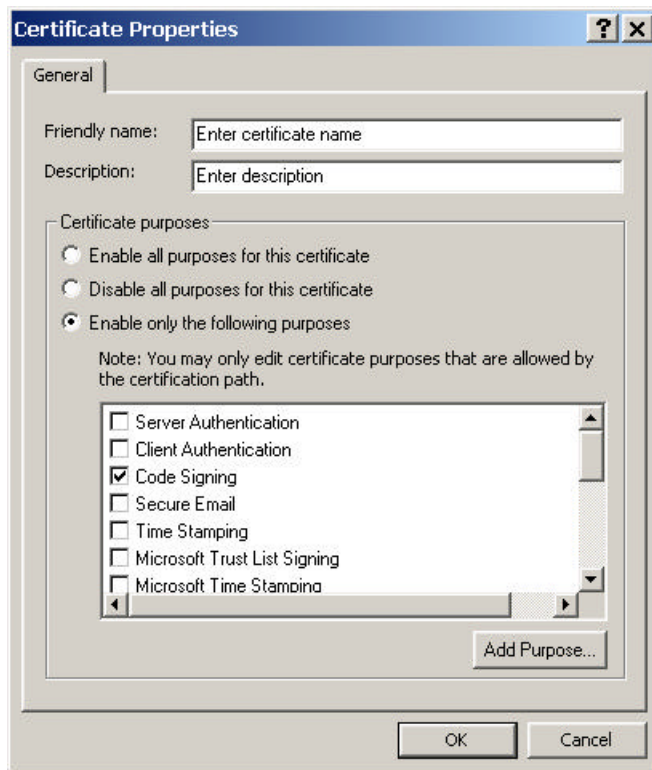


7. Select **Enable only the following purposes**





8. Uncheck all intended purposes except for **Code Signing**. Windows will only use this certificate and any certificates that this CA issues for code signing (and verification).



9. Click **OK** to save the changes.

---

## Exporting Certificates

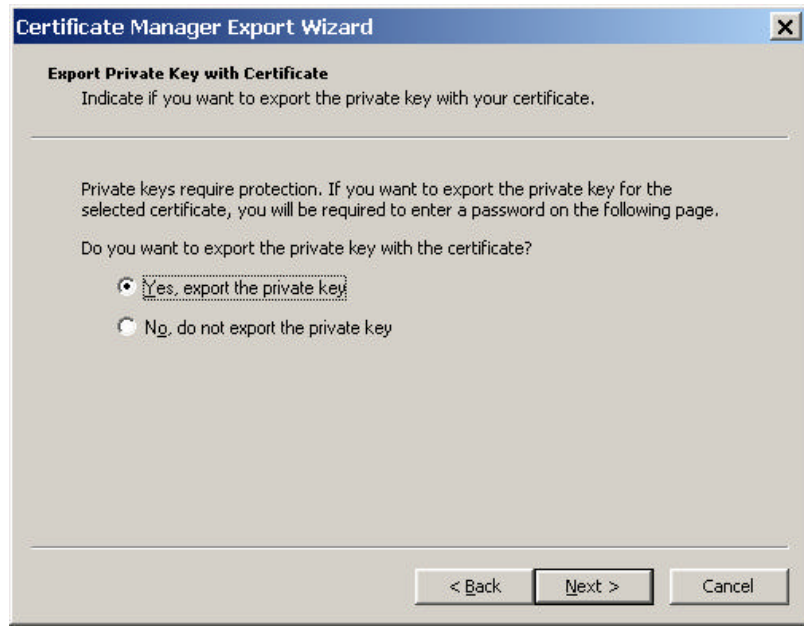
You may backup important certificates and the corresponding private keys, or move them to another computer. To export certificates, do the following:

1. Open **Control Panel**. Start **Certificate Manager** by double-clicking **Users and Passwords**.
2. Select the certificate(s) that you want to export. You may select one or more certificates.
3. Click **Export** to start the **Certificate Manager Export** wizard. Click **Next**.

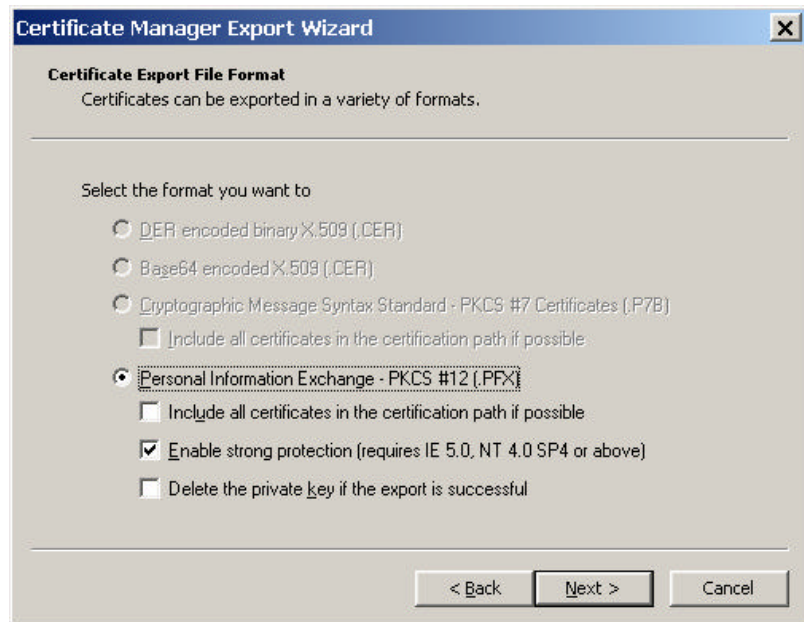


4. If one or more certificates that you are exporting have corresponding private keys in the system, you can choose to export the private keys with the certificates.

**Note** You will only be able to export to a Personal Information Exchange PKCS#12 file if you want to export the private key.



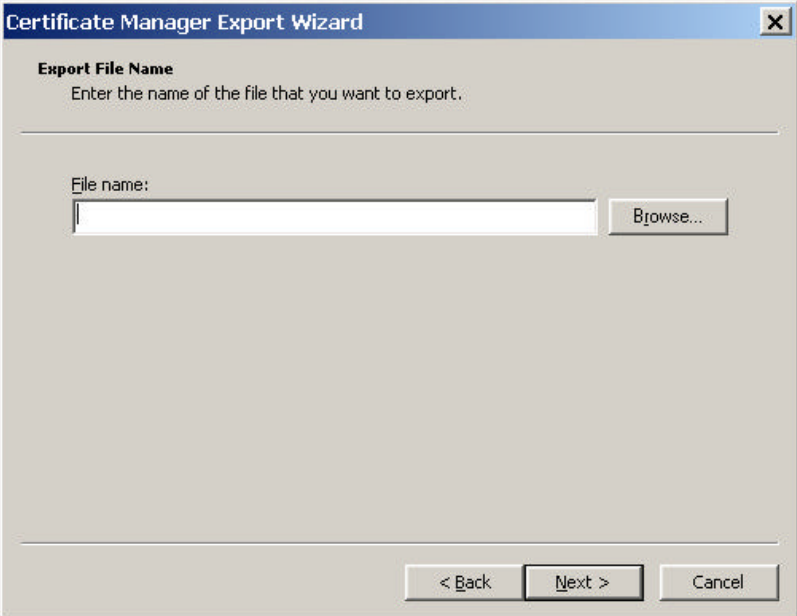
5. Select the export file format and options. Click **Next**.



6. If the file specified is a Personal Information Exchange–PKCS #12 (\*.pfx) file, you will be prompted for the password. You will have to enter the password to import the file later. Click **Next**.



7. Enter the name of the file you want to export. Click **Next**.



The image shows a Windows dialog box titled "Certificate Manager Export Wizard". The dialog has a blue title bar with a close button (X) in the top right corner. The main area is light gray. At the top, it says "Export File Name" in bold, followed by the instruction "Enter the name of the file that you want to export." Below this is a horizontal line. Under the line, the text "File name:" is followed by a text input field. To the right of the input field is a "Browse..." button. At the bottom of the dialog, there are three buttons: "< Back", "Next >", and "Cancel". The "Next >" button is highlighted with a black border.

8. To complete the export process, verify the choices you have made. Click **Finish** to export to the file.



**Note** You may also export a certificate by dragging the certificate from Certificate Manager to a file folder or the desktop. Certificate Manager will export them as DER encoded X.509 certificates. You can override the default export format by clicking **Advanced** on Certificate Manager.

---

## Importing Certificates

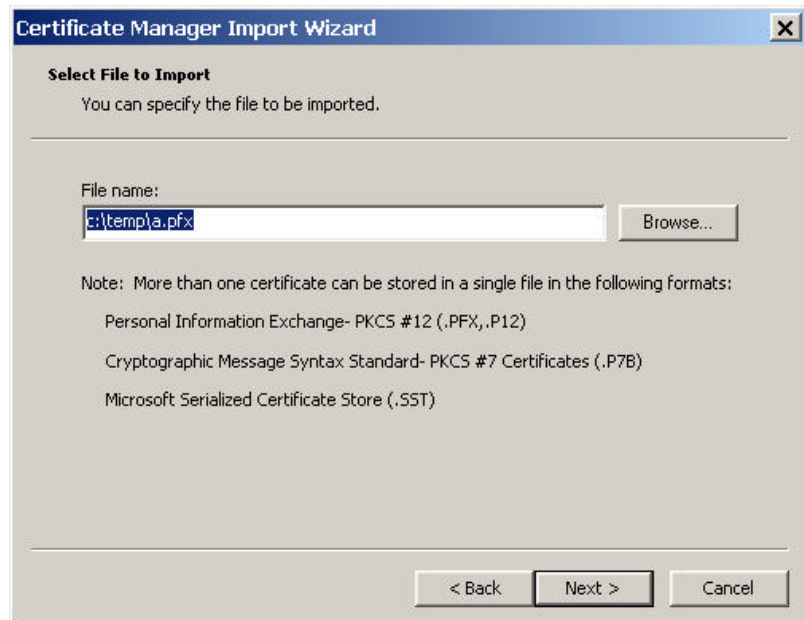
You may restore certificates and the corresponding private keys from a file. To import a file, do the following:

1. Open **Control Panel**. Start **Certificate Manager** by double-clicking **Users and Passwords**.
2. Click **Import** to start the **Certificate Manager Import** wizard. Click **Next**.

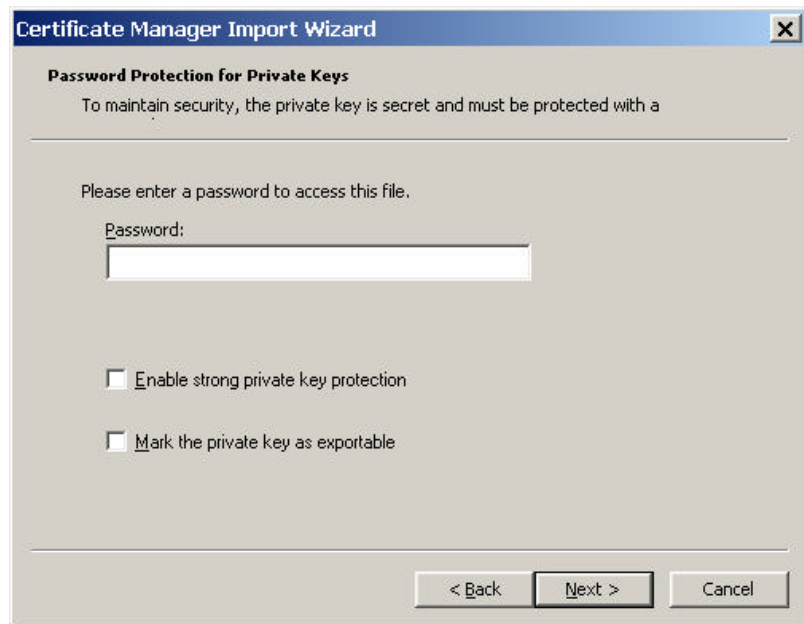




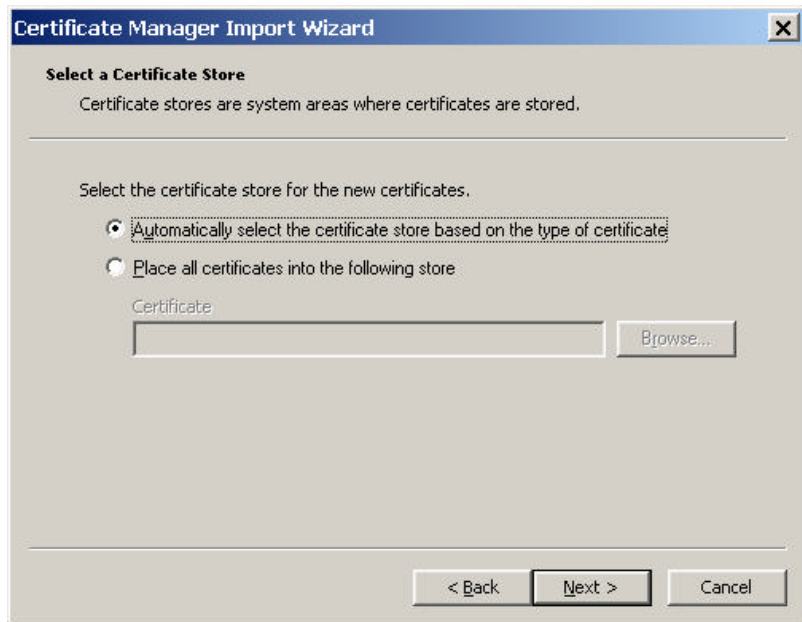
3. Type in the name of the certificate file that you want to import. Alternatively, you may browse to find the file by clicking **Browse**. Click **Next**.



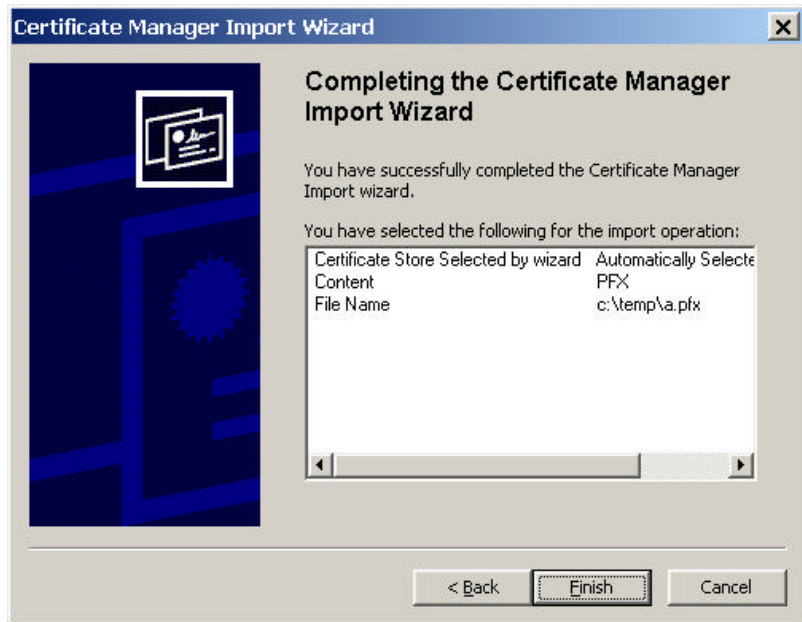
4. If the file specified is a Personal Information Exchange–PKCS #12 (\*.pfx) file, you will be prompted for the password. Enter the password to import the file. Click **Next**.



5. The **Select a Certificate Store** page of the **Certificate Manager Import** wizard allows you to specify the certificate store to import. By default, the wizard imports certificates into the Personal, Intermediate Certification Authorities, and Trusted Root Certification Authorities stores, depending on the information in the certificates being imported. Click **Next**.



6. The **Completing the Certificate Manager Import** wizard page contains summary information about the file that you are importing. Click **Next** to import the file. The certificate(s) are now ready for use by the system.



**Note** You may also import a certificate by dragging the file from a file folder or the desktop to the list. Certificate Manager will place the certificates into the Personal, Intermediate Certification Authorities, and Trusted Root Certification Authorities stores, depending on the information in the certificates being imported.

---

## FOR MORE INFORMATION

For the latest information on Microsoft Windows2000 network operating system, visit our World Wide Web site at <http://www.microsoft.com/windows/server/> and the Windows NT Server Forum on the Microsoft Network (GO WORD: MSNTS).

For the latest information on the Windows2000 Beta 3, visit the World Wide Web site at <http://ntbeta.microsoft.com>.

### Before You Call for Support

Please keep in mind that Microsoft does not support these walkthroughs. The purpose of the walkthroughs is to facilitate your initial evaluation of the Microsoft Windows 2000 features. For this reason, Microsoft cannot respond to questions you might have regarding specific steps and instructions.

### Reporting Problems

Problems with Microsoft Windows 2000 Beta 3 should be reported via the appropriate bug reporting channel and alias. Please make sure to adequately describe the problem so that the testers and developers can reproduce it and fix it. Refer to the Release Notes included on the Windows2000 Beta 3 distribution media for some of the known issues.